In the Specification:

Please amend the specification as follows:

At page 1, lines 9-10

A1

The present invention relates to Internet communication and more particularly to using digital watermarks [to] as control elements in Internet communication.

At page 1, lines 13-20

The Internet presents security challenges to corporations and others who have computers [~~which~~] that store confidential information and [~~which~~] that have connections to the [~~internet~~] Internet. Traditionally, documents containing confidential information are marked with a legend or other visual indicia with words such a "CONFIDENTIAL", "PROPRIETARY", etc. The presence of these marks alert anyone handling such documents that they should only be transferred outside of company under special precautions. It is relatively difficult and unusual for someone to [~~inadvertently~~] manually send such a document to an unauthorized receiver inadvertently. However, the use of Internet communication changes the situation.

A2

At page 1, line 22 through page 2, line 3

The Internet and electronic mail speeds the communications process; however, the Internet and electronic mail also make it much easier to inadvertently or accidentally send a confidential document to an unauthorized receiver. A single [~~accidential~~] accidental or inadvertent keystroke can have wide [~~raging~~] ranging unintended consequences. The Internet and other electronic communication [~~system~~] systems make it easy to communicate; however, these systems and networks also [~~makes~~] make it easy to mistakenly or inadvertently [~~sent~~] send a document to the wrong party.

A3

At page 2, lines 6-11

The present invention utilizes digital watermarks to control the transmission and/or receipt of documents transmitted over computer networks such as the Internet. The invention can be used to prevent the accidental dissemination of information to unauthorized receivers. Furthermore, while no security system is fool-proof, the present invention helps [~~guards~~] guard against the intentional, but unauthorized, dissemination of confidential information to unauthorized receivers.

At page 4, line 19 through page 5, line 11

A typical confidential document 10 is represented in Figure 1. The document 10 can either be an e-mail message, or alternatively it may be a document that is attached to an e-mail message. The document 10 includes a confidentiality stamp 11 and lines of text. The confidentiality stamp 11 is an image that has the word "confidential" superimposed over a background that has a variety of lines. That is, the background in image 11 contains lines the width of which are varied to carry a watermark in accordance with the teachings of US application 09/074,034, filed May 6, 1998, now US Patent 6,449,377, (which corresponds to PCT application PCT/US99/08252 (WO99/53428)), and US application [~~09/127,503~~] 09/127,502, filed July 31, 1998, now US Patent 6,345,104, (which [~~corresponding~~] corresponds to PCT application PCT/US99/14532 (WO00/07356)). The disclosures of the above referenced patent applications are hereby incorporated herein in their entireties by reference. Alternatively the background of image 11 may comprise a weave or tint pattern that carries a watermark. In still another alternative embodiment, instead of having an image 11 embedded in the message, the message may contain an audio clip with the [~~work~~] word confidential. The audio clip would be watermarked using conventional audio watermarking techniques. However, in the first embodiment described herein, the[;] image 11 has both a human readable word "Confidential" and a digital watermark that can be read by a watermark detection and reading program.

At page 6, lines 14-21

A second embodiment of the invention provides for a wider array of [~~alternative~~] alternatives. As shown in Figure 4, the second embodiment of the invention includes a [~~data base~~] database 401. The [~~data base~~] database 401 contains a list of different potential message senders, a list showing different groups of potential message recipients, and a set of possible categories indicated by the setting of the various flags in a message. For example, the senders may fall into three groups designated sender groups S1, S2 and S3. The potential recipients can fall into three groups designated R1, R2, and R3. The [~~data base~~] database 401 and the associated logic 402 can implement logic rules such as indicated by the following table:

At page 7, lines 2-14

It should be clearly noted that the above is merely a simplified example of the rules and combinations that could be in [~~data base~~] database 401. The [~~data bases~~] databases could include hundreds or thousands of users and it could include dozens of rules. The system can be complex or simple as desired for a particular application. A system can include many alternatives in addition to those shown above or a system might include only a very few alternatives. For example, the system could include only a list of addresses which are authorized to receive messages which have a confidentiality flag set to "confidential". Such a system would allow confidential documents to be only sent to selected addresses. Alternatively or in addition the system could include a list of individuals authorized to send confidential documents. The system could merely check the sender against this list or alternatively, the system could require that a password be entered when such messages are encountered. The table above shows only three [~~fag~~] flag bits. A system could have more or less [~~fag~~] flag bits as the needs of the particular system require.